

UNITED STATES DISTRICT COURT

for the
District of Oregon

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)

The property located at 125 North Lane Street, Cottage
Grove, Oregon, as described in Attachment A

Case No. 6:17-MC-601

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

The property located at 125 North Lane Street Cottage Grove, Oregon, including the building, trailers, shipping container style box and a Chevrolet truck, Oregon license plate 536 FTB, as described in Attachment A.

located in the _____ District of _____ Oregon _____, there is now concealed (identify the person or describe the property to be seized):

The information and items set forth in Attachment B hereto.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

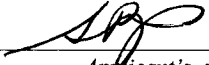
- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
21 U.S.C. § 841(a)(1)	Manufacture of marijuana, and possession with intent to distribute marijuana.

The application is based on these facts:
See affidavit which is attached hereto and incorporated herein by this reference.

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Sean Cummings Special Agent DEA

Printed name and title

Sworn to before me and signed in my presence.

Date: 11/17/2017


Judge's signature

City and state: Eugene, Oregon

Jolie A. Russo, United States Magistrate Judge

Printed name and title

DISTRICT OF OREGON, ss:

AFFIDAVIT OF SEAN CUMMINGS

Affidavit in Support of an Application
Under Rule 41 for a Search Warrant

I, Sean Cummings, being duly sworn, do hereby depose and state as follows:

Introduction and Agent Background

I am a Special Agent with the Drug Enforcement Administration and have been since 1999. My current assignment is at the Eugene Oregon resident Office. My training and experience includes completion of DEA basic training. This training included the investigation, detection, and identification of controlled substances. I have also completed Conspiracy and Complex Investigations training. Additionally I have participated in numerous narcotics investigations since my employment with the DEA as a case agent, undercover agent and surveillance agent. I have consulted and conversed with numerous other agents from various local, state and federal agencies on drug cases of all types including the distribution of marijuana, heroin, cocaine and methamphetamine. As a result of this and my own experience and training, I am familiar with marijuana, heroin, cocaine and methamphetamine and the methods employed by traffickers of these controlled substances.

I submit this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the property located at 125 North Lane Street Cottage Grove, Oregon in Lane County, as described in Attachment A hereto, including the building, trailers and shipping container style

box. One of the trailers is a white enclosed 2018 Forri Cargo Mate trailer bearing Oregon license U523636. Also to be searched is a Chevrolet truck, Oregon license plate 536 FTB, parked in front of the building. Both the truck and the Forri trailer are registered to Walter Andrew LIVINGSTON in Florence, Oregon. As set forth below, I have probable cause to believe that evidence, contraband, fruits, and instrumentalities of violations of 21 U.S.C. §§ 841(a)(1) manufacture of marijuana, and possession with intent to distribute marijuana, as described in Attachment B hereto, including digital devices or electronic storage media, will be located at the building located at 125 North Lane Street Cottage Grove, Oregon.

This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

The facts set forth in this affidavit are based on my own personal knowledge, knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers, State of Oregon Fire Marshals, interviews of witnesses, and others who have knowledge of the events and circumstances described herein, and information gained through my training and experience. Statements of individuals are stated in substance, unless otherwise indicated.

Statement of Probable Cause¹

¹ Based on my training and experience, I use the following technical terms to convey the

1. On November 16, 2017, at about 3:52 p.m., South Lane County Fire Department was dispatched to an explosion at a building located at 125 North Lane Street in Cottage Grove, Oregon. Upon arrival at the scene of the explosion a male was located with burns to his face and hands and he was transported to a Portland area hospital specializing in burned subjects. This subject was identified as Eric Leighton SCULLY. I am familiar with Eric SCULLY as he was prosecuted in federal court in Eugene, Oregon, for 18 U.S.C. § 1957, Money Laundering, as it related to a marijuana cultivation operation in about 2015. SCULLY was sentenced to 90 days in jail in September 2016, reported to jail in January of 2017, was released on March 31, 2017, and was placed on federal supervised release for three years. The State of Oregon Fire Marshal stayed on scene until the Cottage Grove Police was notified. The scene

following meanings:

- a. *IP address.* The Internet Protocol address (or simply “IP address”) is a unique numeric address used by digital devices on the Internet. Every digital device attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that digital device may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some digital devices have static—that is, long-term—IP addresses, while other digital devices have dynamic—that is, frequently changed—IP addresses.

- b. *Internet.* The Internet is a global network of digital devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

- c. *Storage medium.* A storage medium is any physical object upon which data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

was secured and other than fire personnel and law enforcement, no other subjects have entered the building, and the police currently remain on scene securing the building, the truck and the trailer described above.

2. On November 17, 2017, at about 8:00 a.m., Cottage Grove Police Officer Josh Dumas contacted your affiant regarding the building and SCULLY. Officer Dumas told me that the State of Oregon Fire Marshal advised him that there were over two hundred growing marijuana plants inside the building. State prosecution of this matter was declined, and Officer Dumas asked for the Drug Enforcement Administration's assistance due to the quantity of marijuana, the subject being on Federal Supervised Release, and the conversion of the marijuana to extracts by utilizing butane, commonly called Butane Honey Oil (BHO), which was one of the catalysts causing the explosion as determined by the Fire Marshal.
3. At about 9:30 a.m., your affiant responded to 125 North Lane Street in Cottage Grove, Oregon. While there I spoke with the South Lane Fire Marshal Danny Solesbee who indicated that while conducting the fire investigation he saw about two hundred marijuana plants, additional small clone marijuana plants, and about fifty pounds of processed marijuana in various stages. Fire Marshal Solesbee said that it appeared that there was a conversion of marijuana extracts that caused the explosion and burned Eric SCULLY. State Fire Marshal Solesbee showed your affiant several photographs from inside the

building where there were several large fifty five gallon garbage bags he indicated were full of marijuana.

4. Also while on scene, your affiant spoke with Officer Dumas who said he spoke with the Oregon Liquor Control Commission (OLCC) who indicated that a permit had been filed with them but no license was issued for this location for production of marijuana. Officer Dumas asked OLCC if the cultivation or extraction of marijuana was authorized at the location and he was told that it was not authorized. Officer Dumas also spoke with the Oregon Health Authority (OHA) who indicated that there were two patients for this location but their permits as patients expired and the location at 125 North Lane Street was not a licensed marijuana grow location. Officer Dumas asked OHA if the cultivation or extraction of marijuana was authorized at the location and he was told that it was not authorized. I know that even with two licensed patients two hundred mature marijuana plants is more than is allowed under State of Oregon law.
5. Officer Dumas also advised your affiant that there was a large safe located inside the structure and two large enclosed trailers on the property located to the Southwest. Your affiant saw both enclosed trailers and one was identified as bearing Oregon license U523636 registered to Walter Andrew LIVINGSTON in Florence, Oregon. The other trailer had no license. There was also a shipping container type metal storage box located on the West side of the building and a

2006 Chevy Silverado pickup bearing Oregon license 536FTB registered to LIVINGSTON parked in front of the building where the marijuana cultivation operation and BHO lab was located. I spoke with LIVINGSTON and he said that SCULLY is his future son-in-law and he lets SCULLY use his truck and trailer. The property 125 North Lane Street in Cottage Grove is fenced, and it does not appear that any other business is associated with the property.

6. Officer Dumas advised your affiant that there was a security camera and recording system inside the structure, several computers, and other documents.
7. Oregon State Police Detective Travis Neubauer attempted to interview Eric SCULLY but he did not provide a statement and he gave Detective Neubauer his attorney's name. SCULLY also indicated that he would have to consult with another attorney before signing any consent to search forms.
8. On July 12, 2016, while conducting surveillance of a known drug trafficker in another investigation, I saw the trafficker go 125 North Lane Street in Cottage Grove. While the trafficker was there, I saw a vehicle registered to SCULLY's relative at the same building. I know that the quantity of marijuana in the building, both the number of plants and the quantity of processed marijuana, is not personal use quantity but rather possessed for distribution. A pound of indoor-grown marijuana can sell for approximately \$1000 to \$4000 depending on what part of the country it is sold. I also believe that given the scale of the extraction operation, that the marijuana extracts were being produced for

distribution. Accordingly, I believe that a search of the building and the trailer will reveal evidence, contraband and instrumentalities used in the manufacture and distribution of marijuana, including manufacturing paraphernalia, scales, packaging material, currency used to finance the operation and proceeds from marijuana sales, records showing who paid for expenses associated with the operation, records identifying associates of SCULLY, customers, co-conspirators and their communications and location, financial records, and any other locations associated with the operation.

9. As described above and in Attachment B, this application seeks permission to search for records that might be found on the Premises, in whatever form they are found. One form in which the records will likely be found is data stored on a computer's hard drive, on other storage media, or other digital devices, including cell phones (hereinafter collectively referred to as digital devices). Thus, the warrant applied for would authorize the seizure of electronic storage media or the copying of electronically stored information, all under Rule 41(e)(2)(B).
10. There is probable cause to believe, and I do believe, that records will be stored on a digital device because, based on my knowledge, training, and experience, I know:

- a. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a digital device,

deleted, or viewed via the Internet. Electronic files downloaded to a digital device can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. When a person “deletes” a file on a digital device, the data contained in the file does not actually disappear; rather, that data remains on the digital device until it is overwritten by new data. Therefore, deleted files or remnants of deleted files, may reside in free space or slack space—that is, in space on the digital device that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a digital device’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

b. Wholly apart from user-generated files, digital devices—in particular, internal hard drives—contain electronic evidence of how a digital device has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Digital device users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

c. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

11. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant but also for forensic electronic evidence that establishes how digital devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any digital device in the Premises, because, based on my knowledge, training, and experience, I know:

a. Data on the digital device can provide evidence of a file that was once on the digital device but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the digital device that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the digital device was in use. Computer file

systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a digital device can also indicate who has used or controlled it. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, email, email address books, “chat,” instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the digital device at a relevant time. Further, forensic evidence on a digital device can show how and when it was accessed or used. Such “timeline” information allows the forensic analyst and investigators to understand the chronological context of access to the digital device, its use, and events relating to the offense under investigation. This “timeline” information may tend to either inculcate or exculpate the user of the digital device. Last, forensic evidence on a digital device may provide relevant insight into the user’s state of mind as it relates to the offense under investigation. For example, information on a digital device may indicate the user’s motive and intent to commit a crime (e.g., relevant web searches occurring before a crime indicating a plan to commit the same), consciousness of guilt (e.g., running a “wiping program” to destroy evidence on the digital device or password protecting or encrypting such evidence in an effort to conceal it from law

enforcement), or knowledge that certain information is stored on a digital device (e.g., logs indicating that the incriminating information was accessed with a particular program).

c. A person with appropriate familiarity with how a digital device works can, after examining this forensic evidence in its proper context, draw conclusions about how digital devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a digital device that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a digital device is evidence may depend on other information stored on the digital device and the application of knowledge about how a digital device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a digital device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a digital device. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

12. In most cases, a thorough search of the Premises for information that might be stored on a digital device often requires the seizure of the device and a later, off-site review consistent with the warrant. In lieu of removing a digital device from the Premises, it is sometimes possible to image or copy it. Generally speaking, imaging is the taking of a complete electronic picture of the digital device's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the digital device and to prevent the loss of the data either from accidental or intentional destruction. This is true because:

a. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a digital device has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine digital devices to obtain evidence. Digital devices can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Records sought under this warrant could be stored in a variety of formats that may require off-site reviewing with specialized forensic tools. Similarly, digital devices can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the digital device off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

13. *Nature of the examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant for which I apply would permit seizing, imaging, or otherwise copying digital devices that reasonably appear to contain some or all of the evidence described in the warrant and would authorize a later review of the device or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire device, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

14. The initial examination of the digital device will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may

seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

15. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the digital device do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

16. If an examination is conducted, and the digital device does not contain any data falling within the ambit of the warrant, the government will return the digital device to its owner within a reasonable period of time following the search and will seal any image of the digital device, absent further authorization from the Court.

17. The government may retain the digital device as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the digital device and/or the data contained therein.

18. The government will retain a forensic image of the digital device for a

number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

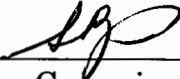
19. The government has made the following prior efforts in other judicial fora to obtain evidence sought under the warrant: None.

Conclusion

20. Based on the foregoing, I have probable cause to believe, and I do believe, that Eric SCULLY committed violations of 21 U.S.C. § 841(a)(1), manufacture of marijuana, and possession with intent to distribute marijuana, and that contraband, evidence, fruits and instrumentalities of those offenses as described above and in Attachment B, are presently located at 125 North Lane Street Cottage Grove, Oregon which is described in Attachment A. I therefore request that the Court issue a warrant authorizing a search of the Premises described in Attachment A for the items listed in Attachment B and the seizure and examination of any such items found.

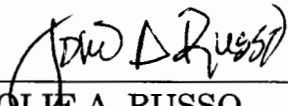
21. Prior to being submitted to the Court, this affidavit, the accompanying application, and the requested search warrant were all reviewed by Assistant United States Attorney (AUSA) Jeffrey Sweet, and AUSA Sweet advised me that in

his opinion the affidavit and application are legally and factually sufficient to establish probable cause to support the issuance of the requested warrant.



Sean Cummings
Special Agent, DEA

Subscribed and sworn to before me this 17th day of November 2017.



JOLIE A. RUSSO
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

The property to be searched is 125 North Lane Street Cottage Grove, Oregon in Lane County, including the building, trailers and shipping container style box. One of the trailers is a white enclosed 2018 Forri Cargo Mate trailer bearing Oregon license U523636. Also to be searched is a Chevrolet truck, Oregon license plate 536 FTB, parked in front of the building. The building is described as a large grey building with blue trim and two man doors to the East and a roll up garage type door to the West. There are no numbers visible on the structure but the warehouse is located on North Lane Street South of Villard Avenue in Cottage Grove, Oregon. See the photographs below for further details.



Front of the building. (East side)



Back of the building (West side)



Trailer



Second trailer (wood and metal)



Shipping container style metal box-brown/rust colored



Truck

ATTACHMENT B

Items to Be Seized

The items to be searched for, seized, and examined, are those items on the property or vehicles, referenced in Attachment A, that contain evidence, contraband, fruits, and instrumentalities of violations of 21 USC § 841(a)(1), manufacture of marijuana, and possession with intent to distribute marijuana. The items to be seized cover the period of July 12, 2016 through the date of the execution of the search warrant.

1. The items referenced above to be searched for, seized, and examined are as follows:
 - a) Controlled substances, specifically marijuana, concentrated cannabis, edibles, and other marijuana products, and residue from controlled substances.
 - b) Drug packaging and distribution materials, mechanical and electronic scales, calibration weights, plastic bags, and plastic wrap.
 - c) Currency and other monetary instruments, U.S. currency, traveler's checks, stored-value cards, and ATM (automated teller machine) cards.
 - d) Drug distribution records, transaction records, ledgers, notes, photographs, videos, receipts, maps, travel documents, address books, and telephone number lists.
 - e) Documents and other items which identify the users, owners, occupants, or associates of the searched property, and their assets, identification documents, bank account records, mail, receipts, account records, tax records, property ownership records, and passwords.

- f) Vehicle keys and records, registration and ownership documents, insurance documents, and maintenance records.
- g) Storage containers capable of storing or concealing drugs or illegal proceeds, and the keys or implements used to access them. The safe can be opened on scene or moved to be opened if necessary.
- h) Financial records including bank statements, cancelled checks, deposit records, check stubs, payment ledgers, checkbook registers, deposit slips, loans, documentation of assets and liabilities, general ledgers, general journals, cash, cash receipts, cash disbursement journals, accounts receivable journals, accounts payable journals, contracts, billing information, and records of bills relating to the receipt of currency or other forms of payment.
- i) Records of credit card and automatic teller machine activity, including credit and/or debit cards, and automatic teller machine records.
- j) Bank statements, canceled checks, duplicate checks, bank deposit records, bank debits, cashier's checks and money order records, and wire transfer records.
- k) Papers, records, documents, files, notes, memos, mail, or other materials representing residency, ownership, occupancy, dominion, or control of the property and structures/vehicles described in Attachment A.
- l) Records showing possession of safe deposit boxes, safes, storage units, and any other type of storage areas, including passwords, keys and/or access codes for access during the searches.

m) Cellular telephones, computers and other electronic devices and digital devices capable of storing data that constitutes evidence or the instrumentality of the manufacture of marijuana and possession with intent to distribute marijuana.

2. As used in this attachment, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form. The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware. The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

3. For any computer or storage medium whose seizure is otherwise authorized by this warrant and any computer, storage medium, or digital device that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter “Computer”):

a. Evidence of who used, owned, or controlled the Computer at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence.

- b. Evidence of software that would allow others to control the Computer, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software.
- c. Evidence of the lack of such malicious software.
- d. Evidence indicating how and when the Computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime under investigation and to the Computer user.
- e. Evidence indicating the Computer user's state of mind as it relates to the crime under investigation.
- f. Evidence of the attachment to the Computer of other storage devices or similar containers for electronic evidence.
- g. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Computer.
- h. Evidence of the times the Computer was used.
- i. Passwords, encryption keys, and other access devices that may be necessary to access the Computer.
- j. Documentation and manuals that may be necessary to access the Computer or to conduct a forensic examination of the Computer.
- k. Records of or information about Internet Protocol addresses used by the Computer.
- l. Records of or information about the Computer's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite"

web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

m. Contextual information necessary to understand the evidence described in this attachment.

Search Procedure

4. The search for data capable of being read, stored, or interpreted by a computer or storage device, may require authorities to employ techniques, including imaging any computer or storage media and computer-assisted scans and searches of the computers and storage media, that might expose many parts of the computer to human inspection in order to determine whether it constitutes evidence as described by the warrant.

5. The initial examination of the computer and storage media will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

6. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the computer and storage media do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the

operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

7. If an examination is conducted, and the computer and storage media do not contain any data falling within the ambit of the warrant, the government will return the computer and storage media to its owner within a reasonable period of time following the search and will seal any image of the computer and storage media, absent further authorization from the Court.

8. The government may retain the computer and storage media as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the computer and storage media and/or the data contained therein.

9. The government will retain a forensic image of the computer and storage media for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.